2016 Defense Health Information Technology Symposium

CCRI Preparation - Panel

DHA Vision

"A joint, integrated, premier system of health, supporting those who serve in the defense of our country."

Learning Objectives

- Learn about the Command Cyber Readiness Inspection (CCRI) program
- Discuss how to prepare for the inspection
- Review CCRI lessons learned
- Provide tips for conducting a Cyber Security Review (CSR)

CCRI - Overview

- ***Command* Cyber Readiness Inspection**
  - Mandated by Instruction
  - Intended to provide Commanders with visibility of key deficiencies in their Cyber Environment
  - Provides USCYBERCOM, JFHQ-DoDIN, DHA and the DoD with increased Cyber situational awareness
  - Currently in CCRI Phase IV: Focus on Operational Risk Assessment & Rapid Adjustment to Ongoing Threats
  - Conducted by DISA Certified CCRI Teams
  - ***Passing score is 70% and above***

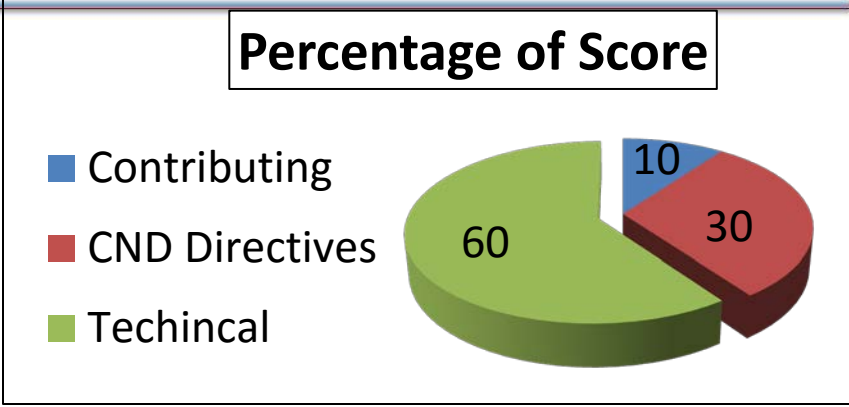
Assessment Areas & Score Breakdown

Contributing – 10%

- Culture, Capability, Conduct

CND Directives – 30%

- CTO 07-015 PKI Phase II, TASKORD 12-0863
- SIPRNet PKI TASKORD 13-670 (ACAS),
- OPORD 12-1016 (HBSS), TASKORD 13-0651 Insider Threat



Technical – 60%

- Network Infrastructure, Domain Name System, Wireless Technologies , Host Based Security System, Traditional Security, Network Vulnerability Scan
- Other Areas: Cross Domain Solutions, Releasable Space (REL), Web Server, Exchange, Video/Voice Over IP, Windows OS

Technical Assessment Areas

- Scored based on the percentage of open findings to potential findings in DISA STIGs
- Conduct self assessment for all applicable STIGs
- Know your score before the inspection
- Each assessed area receives one of the 5 Concern Indicators
- ***60% of Inspection Score***

Technology Areas

Concern Indicator	Threshold
No Downgrade	≥ 30%
Critical Concern	≥ 20% and < 30%
Moderate Concern	≥ 10% and < 20%
Minor Concern	> 0% and < 10%
Minimal Concern	0 CAT Is, <5% II & III
No Concern	0.0%

Technology Areas and Vulnerability Scan	Weight	Concern Indicator	Concern Indicator Value	Weighted Score
Boundary Security	3	Minor Concern	1.0	3.0
Internal Network	3	Minor Concern	1.0	3.0
Combined Vulnerability Scan	4	Minor Concern	1.0	4.0
Domain Name System	3	Minor Concern	1.0	3.0
Host Based Security System	4	Moderate Concern	3.0	12.0
Traditional Security	4	Minor Concern	1.0	4.0
Wireless Communications / Mobility	2	Minor Concern	1.0	2.0
Cross Domain Solution - Admin	2	-		-
Cross Domain Solution - Technical	4	-		-
Exchange	2	-		-
Web Server	3	Minor Concern	1.0	3.0
Database	3	Critical Concern	5.0	15.0
Video and Voice Over Internet Protocol (VVOIP)	2	Minor Concern	1.0	2.0
Windows OS	1	-		-
UNIX OS	1	-		-
Releasable Networks	2	-		-
-- Other Review --	1	-		-

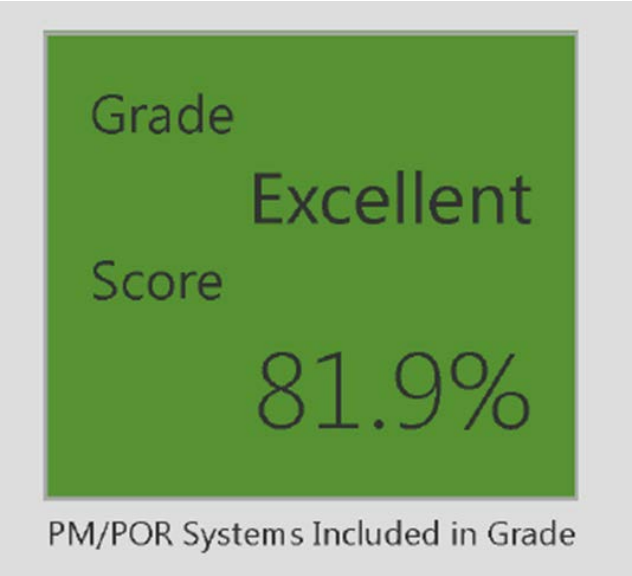
Technical Assessment: Vulnerability Scans

- Build proper Scan Groups (Corporate Assets Workstations, Servers, Network Equipment, Individual POR scans, etc.)
- Build Risk Assessments Report (RAR) POA&M with graph. Identify the System Admin (SA) , total number of assets and assets not scanned. Picture is worth a thousand words.
- Send RAR/Graph to SAs, PMs and supporting Vendors. Accountability. SAs using ACAS, equals IAVM success
- Maintain Nessus files for each system 180 days
- Ensure 100% of assets are able to be scanned and with proper credentials
- Run CCRI-Summary Reports for each Scan to determine concern indicator

Technical Assessment: Manual Reviews

- Ensure STIG compliance for all applicable STIGs for all Technical Assessment Areas
- For example: DNS Technology Area includes:
  - Internal DNS server
  - External DNS server
  - Active Directory forest policy
  - Active Directory Domain policy
  - Underlying operating system STIG
  - IAVMs
  - IE STIG
  - DNS STIG
  - DNS policy
- Refer to CCRI Grading Criteria Worksheet for all STIG details

Post Inspection Actions



- USCYBERCOM TASKORD 14-0290 technical attachment
- Vulnerabilities discovered during CCRI must be addressed / closed:
  - CAT I – 30 Business Days after discovery
  - CAT II / III – 90 Business Days after discovery
- Vulnerability Scan follow up reporting required 15, 30, 45 and 60, 90, 120 days etc. This continues until all CCRI vulnerabilities closed or remediated
- Risk Report Due to USCYBERCOM and JFHQ-DODIN NLT 1200 ET 11.5 business days following Out-brief

Conduct Self Cyber Security Reviews

- Cyber Security Review (CSR) ensures CCRI is not forgotten.
- System Folder, consist of Mission of the system, SA assignment, PM and vendor contacts, System dependency, System diagram, Accreditation status, Cybersecurity Review, Software/Hardware inventory, System ITCP, IRP, IAVM, Access Control List, HBSS and Scans with Graph (present and past for analysis)
- CS Division reviews system folder with latest scans, using CCRI score sheet to determines system status. Implementing CCRI checklist in day to day operations with continue process improvements will ensure success
- CS Division meets with SA and reviews system status. Conducts an ITCP drill and includes PM and Vendor's processes for system failure
- CS Division (ISSM) issues letter of compliance to SA, Ccing CIO, DCIO, Supervisor, and PM. Letter includes action items with due dates.

Summary

- Being prepared will ensure success
- Implementing CCRI and TTP into day to day processes will help ensure a successful inspection
- Evaluate processes to ensure right information supports the task.
- Conduct your own Cyber Security Review

2016 Defense Health Information Technology Symposium

CCRI Preparation - Panel

Objectives

- Develop the baseline
- Develop the game plan
- Share information up and down the chain on a regular schedule

Way Ahead

- Set the baseline
  - Engage local Network Enterprise Center (NEC)
  - Use DISA CCRI Inspection Prep Checklist
  - Gather documentation
  - Begin scan process – all systems need visibility
  - PM systems are critical – engage their PMO early
- Develop game plan
  - Identify key players and assign roles early

Way Ahead

- Use DISA tools: Action Officer CCRI Prep Guide and CCRI Inspection Scoping Worksheet
- DISA CCRI Program page is the definitive source
- Conduct weekly information/progress updates
  - The intent is to show progress from initial state to guaranteed success
  - All stakeholders must be in attendance
  - Leadership involvement is crucial

Summary

- Goal driven process
- Accurate and honest self appraisal is critical to success
- Definitely a team effort

2016 Defense Health Information Technology Symposium

CCRI Preparation - Panel

Learning Objectives

- Identify where to find the information and resources needed to get started
- Develop an iterative process to prepare work stations and servers
- Formulate a plan for local systems

Agenda

- Set the baseline
- Develop game plan
- PMO Systems
- Local Systems

Set the Baseline

- Coordinate with local Base Communications squadron
- Obtain scan results
- Identify your PMO Systems POCs
- Identify local systems (internal & external)
- Verify all systems and PCs have been discovered
- Goal - Score less than 2.5

Develop Game Plan

- Pool human resources
- Assign systems/servers
- Develop a tracking plan - SCCM vs ACAS
- Iterative process, schedule regular progress checks
- Modify work schedules
  - Check contracts

PMO Systems

- #1 Resource - AFMOA/SGALE
  - Reach out and Verify Patch Approvals
  - Final Say on Patch application
- Verify ATO/ATC are On-hand and Current
- POA&Ms up-to-date in eMASS
- Ensure 100% Scan Engine access

Local Systems

- ATO/ATC
- POA&Ms - submitted and approved
- Decide early on - keep them up or shut them down
- Know your alternative patch distribution points
- Ensure 100% scan engine access

Summary

- Long, iterative process
- Incorporate into regular routine
- Ask for help

2016 Defense Health Information Technology Symposium

CCRI Preparation - Panel

CCRI: A DHA Perspective

- DHA Authorizing Official (AO) assumed acceptance of risk for Military Health System (MHS)
- Improved cyber hygiene awareness through trend analysis
- Alignment of results with Risk Management Framework (RMF) Assessment and Authorization (A&A) process
  - Enhance sustainment of cybersecurity posture
  - Authorization to Operate (ATO)

CCRI: A DHA Perspective

- Coordination with cybersecurity operations activities to ensure compliance with:
  - USCYBERCOM Issuances
  - Information Assurance Vulnerability Management (IAVM) program
  - Ports Protocols and Services Management (PPSM)
  - Identity Management implementation
  - Single Cybersecurity Service Provider
    - Common cybersecurity practices across the MHS

CCRI: A DHA Perspective

- DHA, Health Information Technology (HIT) Directorate, Cyber Security Division (CSD), Policy Branch, Compliance/Risk Management Section
  - Responsible for DHA CCRI Program
  - Establish initial coordination with sites
  - Remote support, onsite pre-inspection, onsite during inspection
  - Monitor compliance
  - Analyze lessons learned
  - Facilitate shift from compliance to sustainment focused inspections
  - Conduct trend analysis

Questions?

- **Questions?**

Key Takeaways

- Incorporate CCRI into day to day operations, always examine your processes
  - CSWF
  - ACAS
  - IAVM
  - CCB
  - ITCP
  - IRP
- Cyber Security Review
  - Supports CCRI
  - Opportunity to address issues before it's to late

Key Takeaways

- Defense Information System Agency (DISA)
- https://disa.deps.mil/ext/cop/fs-ccri/inspections/SitePages/Command_Cyber_Readiness_Inspection_(CCRI)_Program.aspx
- https://disa.deps.mil/ext/cop/iase/ttp/operational/Pages/index.aspx
- http://iase.disa.mil/Pages/index.aspx
- https://iavm.csd.disa.mil
- DHA Cyber Security
- https://info.health.mil/hit/infosec/SitePages/Home.aspx

Key Air Force Takeaways

- AFMOA CCRI Preparation Site on the AFMS KX
  https://kx2.afms.mil/kj/kx10/SGAI/Documents/Forms/ShowFolders.aspx?RootFolder=%2Fkj%2Fkx10%2FSGAI%2FDocuments%2FCCRI&undefined
  - Inspection Dates, Lessons Learned, Prep Guide, DISA CCRI Guides
- Local Communications squadron sets the base tone
- AFMOA/SGALE for PMO Systems
- AFMOA Reachback for any questions

Evaluations

Please complete your evaluations

Contact Information

- Mr. Richard Kesterson
- ISSM, NMC San Diego
- richard.k.kesterson.civ@mail.mil

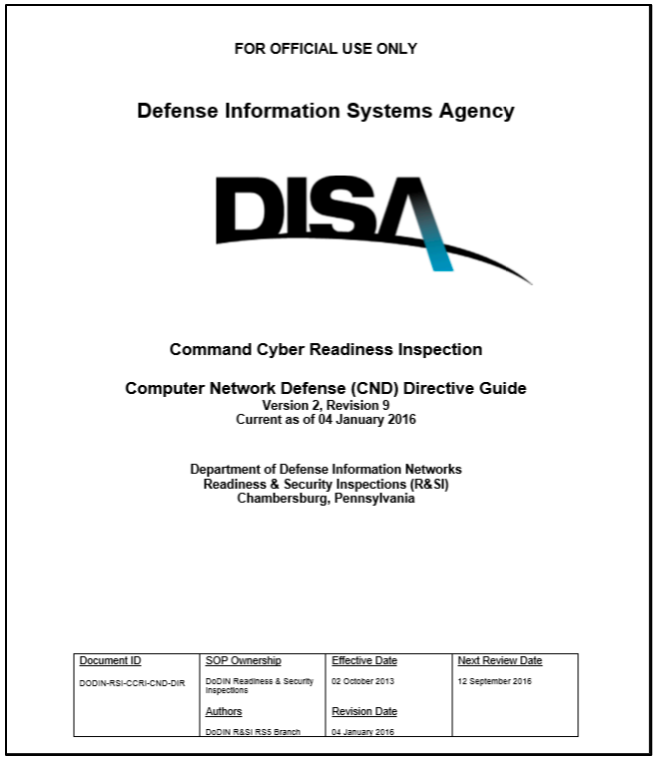
- Lt Col Duane Webster
- CIO, 59 MDW
- duane.webster@us.af.mil

- Mr. Robert F. Rhodes
- CIO, Army Medical Command
- robert.f.rhodes6.civ_mail.mil

- Ms. Joan Luke
- DHA Cyber Security
- joan.r.luke.civ@mail.mil

CND Directives

- **FY16 CND Assessed Directives Include:**
  - CTO 07-015 PKI Phase II (NIPR)
  - TASKORD 12-0863 SIPRNet PKI
  - TASKORD 13-670 (ACAS)
  - OPORD 12-1016 (HBSS)
  - TASKORD 13-0651 Insider Threat
- **CND Directive Guide is updated regularly**
- ***30% of Inspection Score***
- **Receive Ratings of:**
  - Not Compliant
  - Partially Compliant
  - Fully Compliant



FOR OFFICIAL USE ONLY

Defense Information Systems Agency

DISA

Command Cyber Readiness Inspection

Computer Network Defense (CND) Directive Guide
Version 2, Revision 9
Current as of 04 January 2016

Department of Defense Information Networks
Readiness & Security Inspections (R&SI)
Chambersburg, Pennsylvania

Document ID	SOP Ownership	Effective Date	Next Review Date
DODIN-RSI-CCRI-CND-DIR	DoDIN Readiness & Security Inspections	02 October 2013	12 September 2016
	Authors	Revision Date	
	DoDIN R&SI RS5 Branch	04 January 2016	